Journal of Human-centric Research in Humanities and Social Sciences
Vol.6, No.1 (2025), pp.13-26
http://dx.doi.org/10.21742/jhrhss.2025.6.1.02

Balancing Privacy and Progress in Big Data Governance across Jurisdictions

Emily Robertson[1*], Daniel Clarke[2], Jonathan Hughes[3] and Sarah Whitfield[4]

[1,2]Department of Geography and Environment, London School of Economics and Political Science (LSE), United Kingdom, https://orcid.org/0009-0000-4491-2720, https://orcid.org/0000-0001-7847-4562
[3,4]School of Business and Management, University of Manchester, United Kingdom
[1]e.robertson@lse.ac.uk, [2]d.clarke@lse.ac.uk, [3]j.hughes@manchester.ac.uk, [4]s.whitfield@manchester.ac.uk

Abstract

The exponential growth of big data analytics has reshaped sectors ranging from healthcare to urban planning, while intensifying debates on how to safeguard individual privacy without constraining technological innovation. This study conducts a comparative analysis of three major legal frameworks—the European Union's General Data Protection Regulation, the California Consumer Privacy Act, and Singapore's Personal Data Protection Act—to evaluate how each balances data protection with innovation imperatives. Using a mixed-methods approach that combines doctrinal analysis of statutory provisions, quantitative assessment of enforcement outcomes and qualitative insights from semi-structured interviews with data protection officers, the research examines core principles including consent, accountability, transparency, and data minimization, as well as their implications for fields such as artificial intelligence and smart-city development. The findings highlight a shared emphasis on empowering data subjects and strengthening organizational responsibility, while also revealing notable divergences in consent mechanisms, penalty structures, and approaches to emerging technologies. Building on these insights, the paper proposes a harmonized governance model featuring interoperable consent standards, tiered enforcement proportional to organizational scale and potential harm, international data-sharing agreements, and regulatory sandboxes to encourage privacy-enhancing technologies. The study concludes that achieving a sustainable balance between privacy and progress requires adaptive legal instruments, continuous stakeholder engagement, and robust international collaboration to ensure that data-driven innovation advances without undermining fundamental rights.

Keywords: *Big data, Data privacy, Governance, GDPR, CCPA, PDPA, Cross-jurisdictional comparison, Harmonization*

1. Introduction

The rapid rise of big data analytics has opened up unprecedented opportunities across sectors such as healthcare, smart-cities, finance, and urban planning. These opportunities

Article history:
Received (April 18, 2025), Review Result (May 26, 2025), Accepted (June 15, 2025)
*corresponding author

come hand in hand with urgent concerns over individual privacy, data misuse, algorithmic bias, and regulatory fragmentation. The tension between protecting personal data and enabling technological innovation is increasingly central to public policy, law, and organizational strategy.

Over the past few years, scholarship has addressed how regulatory regimes attempt to balance privacy and innovation. Studies have examined dynamic consent models in health research ecosystems [1], enhancements via differential privacy, zero-knowledge proofs, and decentralization to strengthen consent systems [2], comparative analyses of data protection laws across major jurisdictions [3], blockchain-based systems for identity and consent management [4], and how data protection legislation functions in developing regions such as Africa in the context of big data health research [5]. Other research has explored the role of regulatory sandboxes in AI governance [6], examined trustworthiness and privacy-by-design practices in sandbox environments [7], and investigated collective intermediary models—such as data trusts and cooperatives—as alternatives to purely individualist data rights [8]. Additional studies have focused on consent erosion in big data, especially around repurposing data and transparency deficits [9], and the use of ML/NLP methods to compare overlap and conflicts among regulations like GDPR and CCPA [10]. Despite this growing body of work, there remain gaps in how legal frameworks operationalize key governance principles (like consent, accountability, transparency, data minimisation) in relation to emerging technologies and cross-border data flows.

This paper advances the field by performing a comparative legal analysis of three leading regulatory regimes—namely the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Singapore's Personal Data Protection Act (PDPA)—with the aim of developing a harmonised governance model that reconciles privacy protection and innovation across jurisdictions. The specific research problem is: How do the GDPR, CCPA, and PDPA differ in their legal mechanisms for balancing privacy and progress, and what features would a harmonised model need in order to be effective across different legal, technological, and economic environments?

The novelty of this study lies in several contributions:

- integration of doctrinal legal analysis with empirical enforcement data and qualitative interviews with data protection officers, enabling a multidimensional view not often present in existing studies;
- cross-jurisdictional focus combining EU, US (California), and Singapore contexts, with attention to how emerging technologies (e.g., AI, smart-city data systems) challenge existing assumptions;
- proposal of a harmonised governance model, including interoperable consent standards, tiered enforcement, regulatory sandboxes, and international data sharing agreements, which directly responds to the comparative findings.

This study is structured as follows. Section 2 reviews the literature on key governance principles (consent, accountability, transparency, data minimisation) and recent innovations such as dynamic consent, regulatory sandboxes, and collective intermediaries. Section 3 describes the methodology: doctrinal legal analysis, quantitative enforcement outcome comparison, and qualitative interviews. Section 4 presents comparative findings on how GDPR, CCPA, and PDPA address core governance principles and emerging challenges. Section 5 proposes a harmonised governance model informed by those findings and assesses its feasibility. Section 6 discusses limitations, policy implications, and directions for future research. Section 7 concludes, emphasizing how to sustain a balance between privacy and progress as big data governance evolves.

2. Literature review

The governance of big data has emerged as one of the most pressing challenges for policymakers, organisations, and civil society. The exponential increase in data collection, processing, and cross-border transfer has created tensions between enabling technological progress and ensuring the protection of individual rights [12]. Early scholarship emphasised the risks of unregulated data flows, particularly regarding surveillance, profiling, and potential discrimination [13]. More recent work highlights how divergent regulatory approaches create compliance burdens for multinational firms while simultaneously leaving gaps that may undermine effective protection [14]. Comparative studies demonstrate that regional frameworks, such as the European Union's General Data Protection Regulation (GDPR), have influenced global norms, but significant variations persist across jurisdictions like the California Consumer Privacy Act (CCPA/CPRA) and Singapore's Personal Data Protection Act (PDPA) [15][16].

Scholars identify consent, accountability, transparency, and data minimisation as core governance principles that underpin modern data protection frameworks [17]. Consent, while central, has been criticised for fatigue effects and limited effectiveness in addressing opaque or large-scale analytics [18]. Transparency obligations are similarly challenged by the complexity of algorithmic systems, with some researchers arguing that simplified disclosures and layered approaches are necessary to ensure meaningful comprehension [19]. Accountability mechanisms, including Data Protection Impact Assessments (DPIAs), organisational governance, and record-keeping, remain crucial in aligning innovation with responsibility [20]. Studies also highlight the role of enforcement structures, such as fines, audits, and cross-border cooperation mechanisms, in shaping compliance cultures [21].

A growing body of literature underscores the role of sectoral applications of big data in shaping regulatory debates. In healthcare, predictive analytics and personalised medicine promise efficiency gains but raise concerns over sensitive health data, secondary use, and patient consent [22]. In finance, algorithmic trading and credit-scoring models demand robust safeguards against bias and manipulation [23]. In urban planning, smart-city initiatives have produced both significant innovations in traffic management and sustainability, and heightened anxieties about surveillance and control [24]. Comparative research shows that regulatory sandboxes, risk-based assessment models, and privacy-by-design principles have been used to mediate these tensions in practice [25][26].

Recent literature also examines the global dimension of data governance. The extraterritorial reach of the GDPR has created ripple effects across multiple jurisdictions, pushing both harmonisation and fragmentation simultaneously [27]. At the same time, scholars caution that without mechanisms for cross-border interoperability, international data transfers risk being stifled, undermining both commerce and research collaboration [28]. Some proposals advocate for international agreements or model contractual clauses to facilitate data mobility while safeguarding rights [29].

2.1. AI, Large Language Models (LLMs), and privacy

The advent of Artificial Intelligence (AI), particularly large language models (LLMs), introduces new technical and regulatory challenges that amplify long-standing debates in data governance. LLMs, trained on vast amounts of publicly available and proprietary data, risk exposing sensitive information through model memorisation, inversion attacks, or inference-based techniques [30]. Studies reveal that adversaries can query models to extract training data or infer whether specific individuals' data were included in training sets, raising concerns

under GDPR's definition of personal data and CCPA's provisions on sensitive categories [31].

Membership inference and attribute inference attacks have proven particularly problematic, demonstrating that even anonymised datasets may not fully protect individuals when used in model training [32]. This challenges assumptions underpinning current anonymisation standards and complicates compliance with principles of data minimisation and purpose limitation. Other research identifies vulnerabilities at the instruction level, where prompt injection and poisoning of alignment data can cause models to disclose private information or behave contrary to safety measures [33].

Mitigation strategies under active development include differential privacy (DP) during training, which offers provable guarantees of individual protection but often reduces model utility at stricter settings [31][36]. Federated learning and decentralised training paradigms reduce centralised data collection but introduce their own communication and reliability challenges [38]. Red-teaming and adversarial testing, increasingly encouraged by regulators, provide system-level safeguards by identifying vulnerabilities before deployment [34][35]. Yet scholars caution that no technical fix is sufficient in isolation; instead, governance models must integrate technical safeguards with legal obligations and organisational accountability [35].

From a comparative law perspective, GDPR, CCPA, and PDPA differ in their readiness to address these emerging AI-specific risks. While GDPR provides a general framework through concepts like DPIAs and the right to explanation, the CCPA has begun to expand its scope to automated decision-making, and Singapore's PDPA has explored regulatory sandboxes for AI experimentation. Literature suggests that harmonisation efforts should focus on interoperable standards for privacy-preserving AI development, cross-jurisdictional testing benchmarks, and coordinated regulatory guidance [34][37].

In summary, the literature reflects both convergence and divergence in global data governance. While privacy principles remain central, the integration of AI and LLMs presents novel challenges that existing frameworks only partially address. These gaps justify the present study's focus on harmonising big data governance across jurisdictions, with a particular emphasis on ensuring that adaptive legal frameworks keep pace with emerging technologies.

3. Methods

This study investigates the central research problem of how to achieve a sustainable balance between protecting individual privacy and enabling technological innovation within big data governance across jurisdictions. Specifically, it seeks to evaluate whether existing legal frameworks—the General Data Protection Regulation (GDPR) of the European Union, the California Consumer Privacy Act (CCPA), and Singapore's Personal Data Protection Act (PDPA)—offer sufficiently harmonized approaches to address emerging challenges such as artificial intelligence (AI) and large language models (LLMs).

To address this problem, a comparative, mixed-methods approach was employed. The choice of methodology reflects the complexity of the research question, which requires legal analysis, empirical validation, and stakeholder perspectives. This triangulation strengthens the reliability of findings and mitigates the limitations of relying on a single method.

3.1. Research design and approach

The methodological design combined three strands of inquiry:

1. Doctrinal Legal Analysis – A close reading and interpretation of statutory texts, implementing regulations, and regulatory guidance documents from GDPR, CCPA, and PDPA. This strand emphasized core governance principles such as consent, accountability, transparency, and data minimization.
2. Quantitative Assessment – An analysis of enforcement outcomes, including the number, nature, and severity of penalties imposed between 2018 and 2024. This allowed for cross-jurisdictional comparison of how laws are operationalized in practice.
3. Qualitative Inquiry – Semi-structured interviews with 15 data protection officers (DPOs) and compliance managers from the healthcare, finance, and smart-city sectors. This component was designed to elicit practitioner perspectives on governance gaps, enforcement pressures, and the integration of privacy-enhancing technologies.

3.2. Data collection

1. Legal texts and regulatory guidelines were collected from official repositories and government websites to ensure accuracy.
2. Enforcement data was drawn from publicly available databases, including the European Data Protection Board (EDPB) enforcement register, California Attorney General's reports, and Singapore's Personal Data Protection Commission annual reports.
3. Interview data was obtained through purposive sampling of professionals with at least three years of compliance experience. All interviews were conducted virtually, recorded with consent, and transcribed for thematic analysis.

3.3. Data analysis

1. Legal analysis was conducted through thematic coding of governance principles, highlighting areas of convergence and divergence across jurisdictions.
2. Quantitative enforcement data was subjected to descriptive statistical analysis, focusing on trends in frequency, severity, and targeted sectors.
3. Qualitative interview transcripts were analyzed using NVivo software, applying inductive coding to capture emergent themes such as challenges with AI deployment, cross-border data sharing, and regulatory uncertainty.

3.4. Methodological evaluation

The integration of doctrinal, quantitative, and qualitative approaches provided a multi-dimensional understanding of the research problem. While doctrinal analysis offered normative insights, quantitative data provided empirical grounding, and qualitative perspectives enriched the findings with real-world experience. This combination was chosen to increase validity and generate actionable recommendations for harmonized governance.

3.5. Obstacles and solutions

Several obstacles emerged during the research process. First, limited access to enforcement data in some jurisdictions constrained the scope of statistical analysis. This was addressed by supplementing official data with secondary sources, such as independent legal reports and industry white papers. Second, potential biases in qualitative interviews were mitigated through anonymization, triangulation with documentary evidence, and cross-checking findings across multiple respondents. Finally, the rapidly evolving nature of AI regulation posed challenges for drawing definitive conclusions; this was addressed by clearly delimiting the temporal scope of analysis and emphasizing adaptability in the proposed governance model.

4. Results

The findings of this study are presented across three tiers: convergence of governance principles, divergences in enforcement and consent mechanisms, and sector-specific implications for emerging technologies. Each tier directly addresses the research problem of how to balance privacy and innovation across regulatory frameworks.

4.1. Convergence in governance principles

Analysis of statutory provisions confirms a strong degree of convergence across GDPR, CCPA, and PDPA in terms of core governance principles. All three regimes recognize the centrality of consent, accountability, transparency, and data minimization as the foundation for lawful data processing. These shared principles indicate that, despite differences in geographic and cultural contexts, there is a common normative commitment to upholding individual rights and imposing duties on organizations shown in Table 1.

Table 1. Shared Big Data Governance Principles across GDPR, CCPA, and PDPA

Governance Principle	GDPR	CCPA	PDPA
Consent	Required for data processing	Opt-out for sale of data	Consent required unless exceptions apply
Accountability	Explicit organizational duties	General compliance obligations	Organizational accountability framework
Transparency	Detailed disclosure requirements	Notice at collection, disclosure of sales	Requirement to notify individuals of purposes
Data Minimization	Explicit principle	Not expressly codified but implied	Aligned with purpose limitation

Note: Convergence in governance principles across GDPR, CCPA, and PDPA.

Across all regimes, individuals are empowered through rights of access, correction, and erasure, while organizations are expected to integrate privacy safeguards into their operational practices. This shared foundation establishes a baseline for interoperability in cross-border data governance.

4.2. Divergences in enforcement and consent mechanisms

Despite shared principles, significant divergences emerge in enforcement models and consent requirements. Enforcement structures vary from GDPR's centralized supervisory authorities, to CCPA's state-level enforcement, and PDPA's commission-driven oversight. Penalty structures also differ sharply: GDPR imposes the most severe financial penalties, CCPA provides consumer-driven statutory damages, and PDPA applies more moderate fines.

Consent mechanisms illustrate the most fundamental divergence, with GDPR requiring prior opt-in, CCPA relying on opt-out, and PDPA adopting a conditional model that blends consent with statutory exceptions shown in Table 2.

Table 2. Divergences in enforcement and consent mechanisms

Regulatory Feature	GDPR	CCPA	PDPA
Enforcement Authority	Centralized (Data Protection Authorities)	State-level Attorney General	Personal Data Protection Commission
Penalty Structure	Up to 4% of global turnover	Statutory damages (USD $100–$750 per consumer)	Fines up to SGD $1 million
Consent Model	Explicit opt-in	Opt-out for data sales	Consent required, with exemptions

Note: Divergences in enforcement and consent requirements across GDPR, CCPA, and PDPA.

Quantitative analysis of enforcement records demonstrates that GDPR's model results in the highest number of actions taken against organizations of varying scales. In contrast, CCPA enforcement activity is less frequent but focuses on consumer rights in relation to data sales. PDPA maintains fewer enforcement actions overall, reflecting its more cooperative compliance approach.

4.3. Sector-specific impacts on emerging technologies

The study's third tier of analysis examined how governance frameworks address the demands of emerging technologies, including Artificial Intelligence (AI), large language models (LLMs), and smart-city applications. Enforcement data from 2018–2024 indicates that GDPR has the most active enforcement record in AI-related contexts, especially cases involving automated decision-making and algorithmic profiling. CCPA actions are concentrated on firms selling consumer data to train machine learning models, while PDPA actions typically address failures to meet accountability obligations in organizational deployment of IoT and smart-city systems shown in Table 3.

Table 3. Enforcement Actions Related to Emerging Technologies (2018–2024)

Jurisdiction	Total Enforcement Actions	AI-Related Cases	Smart-City/IoT Cases
GDPR (EU)	1,250	210	95
CCPA (California)	540	60	40
PDPA (Singapore)	310	35	20

Note: Enforcement activity concerning emerging technologies across three regulatory regimes (2018–2024).

Qualitative interviews reinforced these findings. Data protection officers (DPOs) consistently identified regulatory uncertainty in applying existing principles to LLMs, particularly around issues of training data provenance, explainability, and cross-border data flows. Respondents under GDPR frameworks reported high compliance costs associated with algorithmic transparency requirements. Under CCPA, organizations expressed concern over consumer opt-out rights affecting machine learning training datasets. Under PDPA, organizations highlighted flexibility in implementation but also noted ambiguity in applying purpose limitation to adaptive AI systems.

Collectively, these findings demonstrate that while governance principles are broadly aligned, enforcement intensity, consent structures, and the handling of AI-specific risks diverge significantly across jurisdictions. These differences directly shape how organizations innovate within healthcare, finance, and urban development sectors.

5. Discussion

This study set out to examine how big data governance frameworks across jurisdictions can harmonize the protection of privacy with the facilitation of technological progress. The research problem was framed around the tension between safeguarding individual rights and enabling innovation, particularly in the context of artificial intelligence and smart-city development. By conducting a comparative analysis of GDPR, CCPA, and PDPA, and integrating doctrinal, quantitative, and qualitative data, the findings provide several insights that contribute to both academic discourse and policy debates.

5.1. Convergence and the basis for harmonization

The results show that GDPR, CCPA, and PDPA converge on key governance principles such as consent, accountability, transparency, and data minimization. This convergence reinforces prior research indicating that data governance regimes, regardless of jurisdiction, share a normative foundation that prioritizes individual autonomy and organizational responsibility [12][13][14][15]. The convergence also establishes a conceptual platform for harmonization, as these principles are universally recognized and can serve as the common denominator for international governance models.

5.2. Divergences and their implications

Despite shared principles, divergences in enforcement mechanisms and consent structures highlight practical barriers to harmonization. GDPR's opt-in consent model and punitive enforcement stand in contrast to CCPA's opt-out approach and consumer-driven damages, while PDPA provides a more flexible accountability framework. These differences align with studies noting that legal regimes are shaped by distinct political, cultural, and economic contexts [16][17][18]. The divergences complicate cross-border data flows and create compliance burdens for multinational organizations, supporting arguments in the literature that regulatory fragmentation undermines efficiency in global data-driven markets [19].

5.3. Sectorial and technological dimensions

The results also demonstrate that governance divergences translate into sector-specific consequences, particularly in healthcare, finance, and smart-city development. GDPR's intensive enforcement has the most pronounced impact on AI adoption, with organizations facing stricter scrutiny of automated decision-making. CCPA prioritizes consumer opt-out rights in ways that directly affect machine learning training datasets, while PDPA emphasizes pragmatic compliance but struggles with the purpose limitation principle when applied to adaptive AI systems. These findings resonate with recent scholarship emphasizing that emerging technologies challenge the adequacy of existing governance structures [20][21].

The sector-specific results also provide empirical confirmation of concerns raised in the literature regarding the governance of large language models (LLMs). Interview data revealed that organizations face uncertainty about applying traditional principles such as consent and transparency to LLM training processes, echoing recent technical studies that highlight risks of data leakage, bias, and lack of explainability [22][23].

5.4. Contributions and novelty

This study advances the literature in three ways. First, it provides a comparative, mixed-methods analysis that integrates doctrinal, quantitative, and qualitative perspectives, addressing the gap in prior work that often relies on single-method approaches. Second, it introduces empirical enforcement data (2018–2024) to quantify how legal principles are applied in practice, offering a rare longitudinal dimension to the analysis. Third, it highlights the intersection of governance principles with AI-specific challenges, a topic that remains underexplored despite its growing urgency.

5.5. Toward harmonized governance

The findings support the argument that harmonization is both necessary and feasible, but only if it builds on shared governance principles while accommodating contextual differences. The study's proposed governance model—which incorporates interoperable consent standards, tiered enforcement proportional to scale and harm, international data-sharing agreements, and regulatory sandboxes for privacy-enhancing technologies—directly addresses the divergences observed in the results. This aligns with calls in the literature for adaptive, flexible, and multi-stakeholder governance models that can evolve with technological change [24][25].

5.6. Policy implications

The comparative findings of this study carry several policy implications for regulators, industry actors, and international organizations.

1. Interoperable Consent Standards
   Given the divergences between opt-in, opt-out and conditional consent mechanisms, policymakers should prioritize the development of interoperable consent standards. This would reduce compliance burdens for multinational organizations and strengthen user autonomy across jurisdictions.
2. Tiered Enforcement Frameworks
   The disproportionate compliance costs faced by small and Medium-Sized Enterprises (SMEs) under punitive regimes suggest the need for tiered enforcement that calibrates penalties to organizational size and potential harm. Such proportionality would maintain deterrence without stifling innovation in emerging firms.
3. International Data-Sharing Agreements
   Cross-border data flows remain a friction point due to fragmented enforcement. Formalized international agreements—anchored in the shared governance principles identified in this study—would streamline global data movement while preserving accountability and privacy.
4. Regulatory Sandboxes for AI and LLMs
   The uncertainty highlighted in relation to AI and LLM governance underscores the need for regulatory sandboxes. These controlled environments would allow organizations to test privacy-enhancing technologies, algorithmic transparency tools, and risk mitigation strategies under regulatory oversight.
5. Continuous Stakeholder Engagement
   The findings demonstrate that sector-specific challenges (e.g., healthcare, finance, smart cities) require tailored solutions. Regulators should therefore establish

mechanisms for continuous engagement with industry, civil society, and technical experts to ensure governance frameworks remain adaptive to technological shifts.

6. Conclusion

This study examined the central challenge of harmonizing big data governance across jurisdictions, focusing on how privacy protection can be safeguarded without constraining technological progress. Through comparative mixed-methods analysis of the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Singapore's Personal Data Protection Act (PDPA), the research provided a multi-dimensional assessment of governance principles, enforcement structures, and sector-specific impacts, particularly in the context of artificial intelligence and large language models.

The findings revealed broad convergence across all three frameworks on foundational principles such as consent, accountability, transparency, and data minimization. At the same time, substantive divergences were evident in consent models, enforcement intensity, and the handling of emerging technologies. GDPR demonstrated the most stringent enforcement and opt-in requirements, CCPA emphasized consumer opt-out rights and statutory damages, and PDPA offered a flexible accountability framework. These differences directly influenced how organizations in sectors such as healthcare, finance, and smart cities implement compliance strategies and innovate with emerging technologies.

By integrating doctrinal, quantitative, and qualitative evidence, the study contributes three key insights: (1) convergence on shared principles offers a foundation for harmonization, (2) divergences in enforcement and consent create practical barriers to interoperability, and (3) sector-specific challenges, particularly in AI and LLM contexts, underscore the need for adaptive governance mechanisms. Based on these insights, the research proposed a harmonized governance model featuring interoperable consent standards, tiered enforcement proportional to scale and harm, international data-sharing agreements, and regulatory sandboxes to manage AI-related risks.

The broader conclusion of this study is that achieving a sustainable balance between privacy and progress requires adaptive, collaborative, and internationally coordinated governance. Legal frameworks must evolve in step with technological innovation, ensuring that data-driven growth does not erode fundamental rights. While no single regime currently offers a complete solution, the shared principles identified across jurisdictions demonstrate that harmonization is both possible and necessary. Future research should extend this analysis to additional jurisdictions, assess the effectiveness of proposed harmonization mechanisms in practice, and explore deeper integration of technical safeguards such as privacy-preserving machine learning and explainability tools.

By bridging legal, empirical, and sectorial perspectives, this study underscores that the path forward lies not in choosing between privacy and innovation, but in designing governance systems that enable both to flourish together.

References

[1] A. R. Lee, D. Koo, I. K. Kim, et al., "Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: A scoping review," BMC Medical Ethics, vol.24, no.107, (2023). DOI:10.1186/s12910-023-00988-9

[2] M. I. Khalid, M. Ahmed, and J. Kim, "Enhancing data protection in dynamic consent management systems: Formalizing privacy and security definitions with differential privacy, decentralization, and zero-knowledge proofs," Sensors, vol.23, no.17, pp.7604, (2022). DOI:10.3390/s23177604

[3] S. Lim and J. Oh, "Navigating privacy: A global comparative analysis of data protection laws," IET Information Security, vol.2025, no.1, pp.5536763, (2024). DOI:10.1049/ise2/5536763

[4] R. D. Garcia, G. Ramachandran, K. Dunnett, R. Jurdak, C. Ranieri, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based privacy applications: An analysis of consent management and self-sovereign identity approaches," arXiv preprint, (2024). Available: https://arxiv.org/abs/2411.16404

[5] N. S. Munung, C. Staunton, O. Mazibuko, et al., "Data protection legislation in Africa and pathways for enhancing compliance in big data health research," Health Research Policy and Systems, vol.22, no.145, (2024). DOI:10.1186/s12961-024-01230-7

[6] OECD, "Regulatory sandboxes in artificial intelligence," OECD Digital Economy Papers, (2023). Available: https://www.oecd.org/en/publications/2023/07/regulatory-sandboxes-in-artificial-intelligence_a44aae4f.html

[7] T. Moraes, "Regulatory sandboxes for trustworthy artificial intelligence – global and Latin American experiences," International Review of Law, Computers & Technology, vol.39, no.1, pp.55–74, (2024). DOI:10.1080/13600869.2024.2351674

[8] J. Duncan, "Data protection beyond data rights: Governing data production through collective intermediaries," Internet Policy Review, vol.12, no.3, (2023). DOI:10.14763/2023.3.1722

[9] A. J. Andreotta, N. Kirkham, and M. Rizzi, "AI, big data, and the future of consent," AI & Society, vol.37, pp.1715–1728, (2022). DOI:10.1007/s00146-021-01262-5

[10] R. Sonani and L. Prayas, "Machine learning-driven convergence analysis in multijurisdictional compliance using BERT and K-means clustering," arXiv preprint, (2025). DOI:10.6084/m9.figshare.28259810

[11] B. M. V. Bernardo, H. S. Mamede, J. M. P. Barroso, and V. M. P. D. Dos Santos, "Data governance & quality management—innovation and breakthroughs across different fields," Journal of Innovation & Knowledge, vol.9, no.4, pp.100598, (2024). DOI:10.1016/j.jik.2024.100598

[12] A. Lavorgna and P. Ugwudike, "The datafication revolution in criminal justice: An empirical exploration of frames portraying data-driven technologies for crime prevention and control," Big Data & Society, (2021). DOI:10.1177/20539517211049670

[13] S. Singler and O. Babalola, "Digital colonialism beyond surveillance capitalism? Coloniality of knowledge in Nigeria's emerging privacy rights legislation and border surveillance practices," Social & Legal Studies, (2025). DOI:10.1177/09646639241287022

[14] L. A. Bygrave, "The 'Strasbourg effect' on data protection in light of the 'Brussels effect': Logic, mechanics and prospects," Computer Law & Security Review, vol.40, pp.105460, (2021). DOI:10.1016/j.clsr.2020.105460

[15] X. Gao and X. Chen, "Understanding the evolution of transatlantic data privacy regimes: Ideas, interests, and institutions," in Proceedings of the European Interdisciplinary Cybersecurity Conference (EICC 2024), Xanthi, Greece, June 5–6, 2024. ACM, New York, NY, USA, 13 pages. DOI:10.1145/3655693.3655720

[16] R. Walters, L. Trakman, and B. Zeller, Data Protection Law: A Comparative Analysis of Asia Pacific and European Approaches. Springer, (2019). UNSW Law Research Paper No.19-78. Available: https://ssrn.com/abstract=3463731

[17] C. Gasimova, "Privacy and transparency in an AI-driven world: Does algorithmic transparency fit on data privacy under GDPR?" SSRN, (2023). Available: https://ssrn.com/abstract=4482889

[18] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, “Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence,” arXiv preprint, (2020). DOI:10.1145/3313831.3376321

[19] B. Aysolmaz, R. Müller, and D. Meacham, “The public perceptions of algorithmic decision-making systems: Results from a large-scale survey,” Telematics and Informatics, vol.79, pp.101954, (2023). DOI:10.1016/j.tele.2023.101954

[20] K. Demetzou, “Data protection impact assessment: A tool for accountability and the unclarified concept of ‘high risk’ in the General Data Protection Regulation,” Computer Law & Security Review, vol.35, no.6, pp.105342, (2019). DOI:10.1016/j.clsr.2019.105342

[21] I. Sivan-Sevilla, “Varieties of enforcement strategies post-GDPR: A fuzzy-set qualitative comparative analysis (fsQCA) across data protection authorities,” Journal of European Public Policy, vol.31, no.2, pp.552–585, (2022). DOI:10.1080/13501763.2022.2147578

[22] I. G. Cohen, “Privacy in the age of medical big data,” Nature Medicine, vol.25, no.1, pp.37, (2019). DOI:10.1038/s41591-018-0272-7

[23] P. Vijayagopal, B. Jain, and S. Ayinippully Viswanathan, “Regulations and Fintech: A comparative study of the developed and developing countries,” Journal of Risk and Financial Management, vol.17, no.8, pp.324, (2024). DOI:10.3390/jrfm17080324

[24] Y. Lim, J. Edelenbos, and A. Gianoli, “What is the impact of smart city development? Empirical evidence from a smart city impact index,” Urban Governance, vol.4, no.1, pp.47–55, (2024). DOI:10.1016/j.ugj.2023.11.003

[25] J. Srouji and T. Mechler, “How privacy-enhancing technologies are transforming privacy by design and default: perspectives for today and tomorrow,” Journal of Data Protection & Privacy, vol.3, no.3, (2020). DOI:10.69554/XPTR8215

[26] A. Alaassar, A. Mention, and T. H. Aas, “Exploring how social interactions influence regulators and innovators: the case of regulatory sandboxes,” Technological Forecasting and Social Change, vol.160, pp.120257, (2020). DOI:10.1016/j.techfore.2020.120257

[27] A. Bradford, The Brussels Effect: How the European Union Rules the World. Oxford University Press, New York, (2020). DOI:10.1093/oso/9780190088583.001.0001

[28] V. Lehdonvirta, B. Wú, and Z. Hawkins, “Weaponised interdependence in a bipolar world: How economic forces and security interests shape the global reach of US and Chinese cloud data centres,” Review of International Political Economy, pp.1–26, (2025). DOI:10.1080/09692290.2025.2489077

[29] L. Belli, W. B. Gaspar, and S. Singh Jaswant, “Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries,” Computer Law & Security Review, vol.54, pp.106017, (2024). DOI:10.1016/j.clsr.2024.106017

[30] M. Ko, M. Jin, C. Wang, and R. Jia, “Practical membership inference attacks against large-scale multi-modal models: a pilot study,” in Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV 2023), Paris, France, 2023, pp.4848–4858. DOI:10.1109/ICCV51070.2023.00449

[31] J. Flemings, M. Razaviyayn, and M. Annavaram, “Differentially private next-token prediction of large language models,” arXiv preprint, (2024). Available: https://arxiv.org/abs/2403.15638

[32] N. Carlini, J. Hayes, M. Nasr, M. Jagielski, V. Sehwag, F. Tramèr, B. Balle, D. Ippolito, and E. Wallace, “Extracting training data from diffusion models,” arXiv preprint, (2023). Available: https://arxiv.org/abs/2301.13188

[33] Z. Shao, H. Liu, J. Mu, and N. Z. Gong, “Enhancing prompt injection attacks to LLMs via poisoning alignment,” arXiv preprint, (2024). DOI:10.1145/3733799.3762963

[34] L. Ahmad, S. Agarwal, M. Lampe, and P. Mishkin, “OpenAI's approach to external red teaming for AI models and systems,” arXiv preprint, (2025). Available: https://arxiv.org/abs/2503.16431

[35] Information Commissioner’s Office, “Guidance on AI and data protection,” (2024). Available: https://ico.org.uk

[36] X. Li, R. Zmigrod, Z. Ma, X. Liu, and X. Zhu, "Fine-tuning language models with differential privacy through adaptive noise allocation," in Findings of the Association for Computational Linguistics: EMNLP 2024, Miami, Florida, USA, pp.8368–8375. Association for Computational Linguistics, **(2024)**

[37] A. Greenberg, "This prompt can make an AI chatbot identify and extract personal details from your chats," Wired, Nov. 2024. Available: https://www.wired.com/story/ai-imprompter-malware-llm

[38] N. Truong, K. Sun, S. Wang, F. Guitton, and Y. Guo, "Privacy preservation in federated learning: an insightful survey from the GDPR perspective," Computers & Security, vol.110, pp.102402, (2021). DOI:10.1016/j.cose.2021.102402

This page is empty by intention.